PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-344925

(43)Date of publication of application : 14.12.1999

---

(51)Int.Cl. G09C 1/00
H04L 9/14
H04L 9/34

---

(21)Application number : 10-166004 (71)Applicant : NEC CORP

(22)Date of filing : 29.05.1998 (72)Inventor : KITAMOTO YOHEI

---

(54) PARTIAL CIPHERING DEVICE AND RECORDING MEDIUM READABLE BY COMPUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a partial ciphering device capable of more finely specifying a point to be ciphered in a series of data.

SOLUTION: An information frame having a data part 200 and a ciphering control information part 100 including one or more pieces of ciphering point specification information 103-1, 103-2, in which a starting position of the data to be ciphered among a series of the data stored in the data part 200 and its length are specified and its number 104 is inputted by the partial ciphering device. And an information frame having a data part 400 in which only the data at the point specified by the ciphering control information part 100 among a series of the data is ciphered and a decoding control information part 300 in which the number of pieces of the data to be decoded, its

starting position and length are specified among a series of the data stored in the data part 400 is generated and outputted.

LEGAL STATUS [Date of request for examination] 29.05.1998
[Date of sending the examiner's decision of rejection] 13.11.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] An input means to input the information frame which has the encryption control information section which specified the starting position of the data which serve as a candidate for encryption among a series of data stored in data division and these data division, and its die length, The decryption control information section which specified the starting position of the data which serve as a candidate for a decryption among a series of data stored in the data division which enciphered only the data of the part specified in said encryption control information section among said a series of data, and these data division, and its die length Partial encryption equipment characterized by having the encryption control means which generates the information frame which it has, and an output means to output said generated information frame.

[Claim 2] Partial encryption equipment according to claim 1 characterized by including one encryption part assignment information that the encryption control information section of the information frame inputted with said input means specified the starting position of the data used as the candidate for encryption, and its die length.

[Claim 3] Partial encryption equipment according to claim 1 characterized by including the number of one or more encryption part assignment information that the encryption control information section of the information frame inputted with said input means specified the starting position of the data used as the candidate for encryption, and its die length, and this encryption part assignment information.

[Claim 4] Partial encryption equipment according to claim 2 or 3 characterized by having the cryptographer stage which enciphers the data used as the candidate for encryption to the data of the same size.

[Claim 5] Partial encryption equipment according to claim 2 or 3 characterized by having the cryptographer stage which enciphers the data used as the candidate for encryption to data with bigger size than it.

[Claim 6] Said input means is partial encryption equipment according to claim 4 or 5 characterized by having the configuration which inputs an information frame from the user program of the arbitration of two or more user programs which work on an information processor.

[Claim 7] An input means to input the information frame which has the encryption control information section which specified the starting position of the data which serve as a candidate for encryption among a series of data in which the information processor was stored by data division and these data division, and its die length, The decryption control information section which specified the starting position of the

data which serve as a candidate for a decryption among a series of data stored in the data division which enciphered only the data of the part specified in said encryption control information section among said a series of data, and these data division, and its die length The computer-readable record medium which recorded the program which considers as the encryption control means which generates the information frame which it has, and an output means to output said generated information frame, and is operated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the partial encryption equipment which has the function which enciphers only the part where it was specified more of a series of data as the detail about encryption equipment.

[0002]

[Description of the Prior Art] The data encryption is carried out in order to prevent secret leakage, when transmitting and receiving data between the information processors connected by the communication line. It is divided roughly into the common key system which uses a common key, and the public key system which uses a public key by the class of key used for the cipher system of data, and is divided roughly into the cipher system which is before and after encryption and serves as the

same size with the data size before and behind encryption, and the cipher system which data size expands by encryption. The more the data length which serves as a candidate for encryption by any method becomes long, the more there is instead of [no] in taking much time amount by encryption processing.

[0003] Then, when the difference in significance is among two or more data transmitted to coincidence, the other data can consider shortening the encryption processing time by transmitting as it is by enciphering only data with a high significance. For example, there are two user programs A and B on an information processor, and user-program A transmits a series of data which contain three kinds of data called a1, a2, and a3 by one transmission as shown in drawing 20 (a). User-program B transmits a series of data which contain two kinds of data called b1 and b2 by one transmission, as shown in drawing 20 (b), and it presupposes that data a2 and data b2 are extra sensitive information. In this case, user-program A enciphers only data a2 after generating single string data which consist of data a1, a2, and a3, re-creates single string data by obtained code data a2' and the remaining data a1 and a3, and transmits to partner equipment. Only data b2 are enciphered after generating similarly single string data which consist of data b1 and b2, single string data are re-created by obtained code data b2' and the remaining data b1, and user-program B also transmits to partner equipment. By carrying out like this, the time amount which encryption processing takes can be shortened compared with enciphering the whole (a1-a3, b1-b2) data.

[0004] However, with the configuration that each user program carries out the above partial encryption processings, the load of each user program becomes large too much. In order to solve such a problem, the partial encryption equipment which has the function which enciphers the part where it was specified of a series of data is required.

[0005] The conventional technique applicable to such partial encryption equipment is indicated by JP,2-188782,A. The encryption equipment indicated by this official report receives as a parameter the location on the message which starts the message storing region address, message length, and cipher processing etc., and carries out encryption processing. As for the location on the message which starts cipher processing, the starting position of a communication message is usually specified, and according to assignment of this parameter, encryption equipment does not encipher a communication link header unit, but enciphers only the communication message section.

[0006]

[Problem(s) to be Solved by the Invention] If the conventional encryption equipment

mentioned above is applied, in user-program B mentioned above, single string data which enciphered only data b2 can be obtained by specifying the head of data b2 as a starting position, and notifying to encryption equipment after generation of the data b1 shown in drawing 20 (b), and single string data which consist of data b2. However, since the data a2 to encipher in user-program A mentioned above as shown in drawing 20 (a) are located in the middle, when they specify the head of data a2 as a starting position and notify it to encryption equipment, they have the problem that not only the data a2 but the consecutive data a3 will be enciphered.

[0007] Then, the purpose of this invention is to offer the partial encryption equipment which can specify more finely the part which wants to encipher in a series of data.

[0008]

[Means for Solving the Problem] An input means to input the information frame which has the encryption control information section which specified the starting position of the data with which the partial encryption equipment of this invention serves as a candidate for encryption among a series of data stored in data division and these data division, and its die length, The decryption control information section which specified the starting position of the data which serve as a candidate for a decryption among a series of data stored in the data division which enciphered only the data of the part specified in said encryption control information section among said a series of data, and these data division, and its die length It has the encryption control means which generates the information frame which it has, and an output means to output said generated information frame.

[0009] A configuration including one encryption part assignment information specified the starting position of the data used as the candidate for encryption and its die length is sufficient as the encryption control-information section of the information frame inputted with said input means, and the configuration containing the number of one or more encryption part assignment information and this encryption part assignment information which specified the starting position of the data used as the candidate for encryption and its die length is used. Moreover, a means to encipher the data used as the candidate for encryption is arbitrary, and can adopt a common key system, a public key system, the cipher system enciphered to the data of the same size, and the cipher system enciphered to data with more big size. Furthermore, the partial encryption equipment of this invention can use an input means now in common by two or more user programs in inputting an information frame from the user program of the arbitration of two or more user programs which work on an information processor.

[0010]

[Embodiment of the Invention] Next, the example of the gestalt of operation of this invention is explained to a detail with reference to a drawing.

[0011] Drawing 1 is the block diagram showing an example of the information processor which applied this invention. The information processor 1 of this example is connected with other information processors (not shown) through the communication line 2, and it has two or more user programs 3-1 - 3-m, the data transmitter-receiver 4, and the partial encryption equipment 5 and the partial decryption equipment 6 concerning this invention. Moreover, 7 is the record medium which can machine read CD-ROM, a magnetic disk, semiconductor memory, etc., the program recorded here is read by the information processor 1, and partial encryption equipment 5 and partial decryption equipment 6 are realized on an information processor 1 by controlling actuation of an information processor 1.

[0012] Each user program 3-1 - 3-m send out the information frame which has the encryption control information section which specified the starting position of the data division which stored those data, and the data which serve as a candidate for encryption among a series of data stored in these data division, and its die length to partial encryption equipment 5 with the information on the destination, and the information on delivery origin, when transmitting a series of data to other information processors. The data division which enciphered only the part which partial encryption equipment 5 should analyze the encryption control information section of the information frame inputted from a user program 3-1 - 3-m, and should encipher in data division, The information frame which has the decryption control information section which specified the starting position of the data which serve as a candidate for a decryption among a series of data stored in these data division, and its die length is generated, and it sends out to the data transmitter-receiver 4 with the information on the destination, and the information on delivery origin. The data transmitter-receiver 4 adds the information on delivery origin etc. to the inputted information frame, and transmits to the other information processors of the destination through a communication line 2.

[0013] On the other hand, the data transmitter-receiver's 4 reception of the information frame which was similarly created with other information processors and has been sent through a communication line 2 sends out the information frame to partial decryption equipment 6 with the information on the destination, and the information on delivery origin. Partial decryption equipment 6 analyzes the decryption control-information section of the information frame which inputted from the data

transmitter-receiver 4, generates the information frame which has the encryption control-information section which specified the starting position of the data division which decrypted only the part which should decrypt in data division, and the data which serve as a candidate for encryption among a series of data stored in these data division, and its die length, and sends it out with the information on delivery origin to the user program 3-1 of the destination - 3-m. In addition, the encryption control information section may omit.

[0014] Drawing 2 is the block diagram showing the example of a configuration of partial encryption equipment 5. The partial encryption equipment 5 of this example consists of the input means 51, an encryption control means 52, a cryptographer stage 53, and an output means 54. The input means 51 will pass it to the encryption control means 52, if an information frame is inputted from the user program 3-1 of arbitration - 3-m. The encryption control means 52 analyzes the encryption control information section of an information frame. The data division which enciphered only the data of the part specified in the encryption control information section among a series of data stored in data division in the cryptographer stage 53, and used the other part as data with origin, The information frame which has the decryption control information section which specified the starting position of the data which serve as a candidate for a decryption among a series of data stored in these data division, and its die length is generated. The output means 54 attaches the information on destination [into which the information frame generated by the encryption control means 52 was inputted from a user program 3-1 - 3-m at the time of the input of an information frame], and delivery origin, and sends it out to the data transmitter-receiver 4.

[0015] Drawing 3 is the block diagram showing the example of a configuration of partial decryption equipment 6. The partial decryption equipment 6 of this example consists of the input means 61, a decryption control means 62, a decode means 63, and an output means 64. The input means 61 will pass it to the decryption control means 62, if an information frame is inputted from the data transmitter-receiver 4. The decryption control means 62 analyzes the decryption control information section of an information frame. The data division which decrypted only the data of the part specified in the decryption control information section among a series of data stored in data division with the decode means 63, and used the other part as data with origin, The information frame which has the encryption control information section which specified the starting position of the data which serve as a candidate for encryption among a series of data stored in these data division, and its die length is generated. The output means 64 attaches the information on the delivery origin into which the

information frame generated by the decryption control means 62 was inputted from the data transmitter-receiver 4 at the time of the input of an information frame, and sends it out to the user program 3-1 of the destination - 3-m.

[0016]

[Example] Next, the example of this invention is explained to a detail with reference to a drawing. The following are taken up as an example.

(1) Explain the case where the part which carries out example (2) encryption which can two or more specify the part to encipher is not expanded with the case where data size is expanded by encryption, about the example which can be specified one, and its each (that is, when becoming the same size).

[0017] (1) Example drawing 4 (a) which can two or more specify the part to encipher is drawing showing the example of a format of the information frame inputted into partial encryption equipment 5 from a user program 3-1 - 3-m. The information frame of this example consists of the encryption control information section 100 and data division 200 which consist of two or more user data. The encryption control information section 100 contains one or more encryption part assignment information 103 that the starting position 101 of the data which serve as a candidate for encryption among a series of user data stored in data division 200, and its byte count 102 were specified, and the number 104 of this encryption part assignment information 103, as shown in drawing 4 (b). The size of a starting position 101, a byte count 102, and the number 104 is a fixed length. The relation of a starting position 101 and a byte count 102, and user data and the relation of the number 104 and the encryption part assignment information 103 are shown in drawing 4 (c). As a starting position 101, it is expressed by the byte count to the head cutting tool of the user data concerned at the time of making the 1-byte (that is, head cutting tool of the number 140) eye of the head of an information frame into the 0th byte, for example. In addition, in this example, the information frame inputted into a user program 3-1 - 3-m from partial decryption equipment 6 is also made into the format of drawing 4 (a).

[0018] On the other hand, drawing 4 (d) is drawing showing the example of a format of the information frame inputted into the data transmitter-receiver 4 from partial encryption equipment 5. The information frame of this example consists of the decryption control information section 300 and data division 400 which consist of two or more user data. The decryption control information section 300 contains one or more decryption part assignment information 303 that the starting position 301 of the data which serve as a candidate for a decryption among a series of user data stored in data division 400, and its byte count 302 were specified, and the number 304 of this

decryption part assignment information 303, as shown in drawing 4 (e). The size of a starting position 301, a byte count 302, and the number 304 is a fixed length. As a starting position 301, it is expressed by the byte count to the user data concerned at the time of making the 1-byte (that is, head cutting tool of the number 304) eye of the head of an information frame into the 0th byte, for example. In addition, in this example, the information frame inputted into partial decryption equipment 6 from the data transmitter-receiver 4 is also made into the format of drawing 4 (d).

[0019] (A) It is [0020] when data size is expanded by encryption. (a) An example of processing of the partial encryption equipment 5 in ******** is shown in the flow chart of drawing 5 . If the information frame of a format as shown in drawing 4 (a) from which user program 3-1 - 3-m is sent, the input means 51 will input it (step S1), and it will transmit to the encryption control means 52. The encryption control means 52 analyzes the encryption control information section 100 of an information frame (step S2), and sets an analysis result as a control table (step S3).

[0021] For example, the data division 200 which contain five user data U1, U2, U3, U4, and U5 which are 32 bytes, 32 bytes, 16 bytes, 16 bytes, and 16 bytes respectively as shown in drawing 6 , In the case of the information frame which consists of two encryption part assignment information 103-1,103-2 that the user data U1 and U3 were specified as a candidate for encryption, and the encryption control information section 100 containing the number "2" If the number, a starting position, and the size of a byte count are for example, 1-byte immobilization The 5-37th byte of user data U1 and the 69-85th byte of user data U3 are data for encryption from the head of an information frame. From the user data U2 between the user data U1 and the user data U3, and the user data U3, since back data (user data U4 and U5) are not data for encryption For example, the control table 900 with four entries E1, E2, E3, and E4 as shown in drawing 7 is generated, and a starting position, a byte count, and the value illustrated in the column of the existence of encryption, respectively are set up. In addition, at this time, the column of the starting position after encryption and the byte count after encryption is NULL.

[0022] next, the entries E1 and E from which, as for the encryption control means 52, the column of the existence of encryption of the control table 900 is "**" -- the data of the corresponding part are taken out from data division 200 for every three, and it enciphers by giving the cryptographer stage 53 (step S4).

[0023] Next, the encryption control means 52 sets the data size after encryption as the column of the byte count after encryption of entries E1 and E3, as shown in drawing 7 , and it sets a value as the column of the starting position after encryption

based on it (step S5). For example, since the byte count after encryption of an entry E1 was expanded to "48", the starting position after encryption of an entry E2 is set as "53."

[0024] The encryption control means 52 the number "2" of the entries E1 and E3 from which the column of the existence of encryption of the control table 900 of drawing 7 is "**" Next, the group of the number 304, and the starting position after encryption of an entry E1 "5" and the byte count after encryption "48", The decryption control information section 300 which made the group of the starting position after encryption of an entry E3 "85" and the byte count after encryption "24" the decryption part assignment information 303-1,303-2, respectively is generated (step S6). Thereby, the decryption control information section 300 shown in drawing 6 (b) is generated.

[0025] Next, from the entry E1 of the control table 900 of drawing 7 , the encryption control means 52 will stuff into order the original data on the input frame specified in the column of the starting position of the control table 900, and the column of a byte count in the data after encryption if it is "nothing" sequentially from the head of data division, if the column of the existence of encryption of the entry to an entry E4 is "**", and it generates data division 400 (step S7). Thereby, the data division 400 shown in drawing 6 (b) are generated.

[0026] If the information frame which consists of the decryption control information section 300 and data division 400 as mentioned above is generated, the output means 54 will send an information frame to the data transmitter-receiver 4 with the information on destination and delivery origin (step S8).

[0027] (b) An example of processing of the partial decryption equipment 6 in ******** is shown in the flow chart of drawing 8 . If the information frame of a format as shown in drawing 4 (d) from the data transmitter-receiver 4 is sent, the input means 61 will input it (step S11), and it will transmit to the decryption control means 62. The decryption control means 62 analyzes the decryption control information section 300 of an information frame (step S12), and sets an analysis result as a control table (step S13).

[0028] For example, when the inputted information frame is an information frame shown in drawing 6 (b), 5-53rd byte [the head of an information frame to] user data U1', and the 85-109th byte of user data U3 -- ' -- the data for a decryption -- it is -- a user -- data -- U -- one -- ' -- a user -- data -- U -- three -- ' -- between -- a user -- data -- U -- two -- a user -- data -- U -- three -- ' -- back -- data (user data U4 and U5) -- a decryption -- an object -- data -- it is not -- since -- For

example, the control table 901 with four entries E1, E2, E3, and E4 as shown in drawing 9 is generated, and a starting position, a byte count, and the value illustrated in the column of the existence of a decryption, respectively are set up. In addition, at this time, the column of the starting position after a decryption and the byte count after a decryption is NULL.

[0029] next, the entries E1 and E from which, as for the decryption control means 62, the column of the existence of a decryption of the control table 901 is "**" -- the data of the corresponding part are taken out from data division 400 for every three, and it decrypts by giving the decode means 63 (step S14).

[0030] Next, the decryption control means 62 sets the data size after a decryption as the column of the byte count after a decryption of entries E1 and E3, as shown in drawing 9 , and it sets a value as the column of the starting position after a decryption based on it (step S15). For example, since the byte count after a decryption of an entry E1 is "32", the starting position after a decryption of an entry E2 is set as "37."

[0031] The decryption control means 62 the number "2" of the entries E1 and E3 from which the column of the existence of a decryption of the control table 901 of drawing 9 is "**" Next, the group of the number 104, and the starting position after a decryption of an entry E1 "5" and the byte count after a decryption "32", The encryption control information section 100 which made the group of the starting position after a decryption of an entry E3 "69" and the byte count after a decryption "16" the encryption part assignment information 103-1,103-2, respectively is generated (step S16). Thereby, the encryption control information section 100 shown in drawing 6 (a) is generated.

[0032] Next, from the entry E1 of the control table 901 of drawing 9 , the decryption control means 62 will stuff into order the original data on the input frame specified in the column of the starting position of the control table 901, and the column of a byte count in the data after a decryption if it is "nothing" sequentially from the head of data division, if the column of the existence of a decryption of the entry to an entry E4 is "**", and it generates data division 200 (step S17). Thereby, the data division 200 shown in drawing 6 (a) are generated.

[0033] If the information frame which consists of the encryption control information section 100 and data division 200 as mentioned above is generated, the output means 64 will send to the user program of the destination with the information on delivery origin (step S18).

[0034] (B) It is [0035] when data size is not expanded by encryption. (a) An example of processing of the partial encryption equipment 5 in ******** is shown in the flow

chart of drawing 10 . If the information frame of a format as shown in drawing 4 (a) from which user program 3-1 - 3-m is sent, the input means 51 will input it (step S21), and it will transmit to the encryption control means 52. The encryption control means 52 analyzes the encryption control information section 100 of an information frame, and the number 104 is set as Variable Max and it sets initial value 1 as Variable i (step S22). For example, in the case of the information frame shown in drawing 6 (a), Max is set as 2.

[0036] Next, the encryption control means 52 takes out the data of the part which the encryption part assignment information of eye **** on Variable i shows from the head in the encryption control information section 100 from data division 200 (step S23), and enciphers them by giving the cryptographer stage 53 (step S24). And the original part of data division 200 is overwritten by the generated code data (step S25).

[0037] The processing returned and mentioned now above to step S23 when meaning finishing the processing about one data for encryption, carrying out Variable i +one (step S26) and becoming below Max is repeated. Since processing of all the data for encryption was finished when Variable i was larger than Max, the output means 54 sends out the information frame by which data division were overwritten to the data transmitter-receiver 4 with the information on destination and delivery origin (S28).

[0038] Thus, when data size is not expanded but it becomes the same size by encryption, the contents of the encryption control information section 100 of the inputted information frame are not changed substantially, but serve as the decryption control information section 300 as it is.

[0039] (b) An example of processing of the partial decryption equipment 6 in ******** is shown in the flow chart of drawing 11 . If the information frame of a format as shown in drawing 4 (d) from the data transmitter-receiver 4 is sent, the input means 61 will input it (step S31), and it will transmit to the decryption control means 62. The decryption control means 62 analyzes the decryption control information section 300 of an information frame, and the number 304 is set as Variable Max and it sets initial value 1 as Variable i (step S32). For example, in the case of the information frame shown in drawing 6 (b), Max is set as 2.

[0040] Next, the decryption control means 62 takes out the data of the part which the decryption part assignment information of eye **** on Variable i shows from the head in the decryption control information section 300 from data division 400 (step S33), and decrypts them by giving the decode means 63 (step S34). And the original part of data division 400 is overwritten by the generated decode data (step S35).

[0041] The processing returned and mentioned now above to step S33 when meaning

finishing the processing about one data for a decryption, carrying out Variable i +one (step S36) and becoming below Max is repeated. Since processing of all the data for a decryption was finished when Variable i was larger than Max, the output means 64 sends out the information frame by which data division were overwritten to the user program of the destination with the information on delivery origin (S38).

[0042] Thus, when data are not expanded but it becomes the same size by decryption, the contents of the decryption control information section 300 of the inputted information frame are not changed substantially, but serve as the encryption control information section 100 as it is.

[0043] (2) It is drawing showing the example of a format of the information frame as which the part which carries out a code is inputted into example drawing 12 (a) which can be specified one by partial encryption equipment 5 from a user program 3-1 - 3-m. The information frame of this example consists of the encryption control information section 500 and data division 600 which consist of two or more user data. The encryption control information section 500 consists of one encryption part assignment information 503 that the starting position 501 of the data which serve as a candidate for encryption among a series of user data stored in data division 600, and its byte count 502 were specified. A starting position 501 and the size of a byte count 502 are fixed lengths. The relation of a starting position 501 and a byte count 502, and user data is shown in drawing 12 (b). As a starting position 501, it is expressed by the byte count to the user data concerned at the time of making the 1-byte (that is, head cutting tool of starting position 501) eye of the head of an information frame into the 0th byte, for example. In addition, in this example, the information frame inputted into a user program 3-1 - 3-m from partial decryption equipment 6 is also made into the format of drawing 12 (a).

[0044] On the other hand, drawing 12 (c) is drawing showing the example of a format of the information frame inputted into the data transmitter-receiver 4 from partial encryption equipment 5. The information frame of this example consists of the decryption control information section 700 and data division 800 which consist of two or more user data. The decryption control information section 700 consists of one decryption part assignment information 703 that the starting position 701 of the data which serve as a candidate for a decryption among a series of user data stored in data division 800, and its byte count 702 were specified. A starting position 701 and the size of a byte count 702 are fixed lengths. As a starting position 701, it is expressed by the byte count to the user data concerned at the time of making the 1-byte (that is, head cutting tool of starting position 701) eye of the head of an information frame into

the 0th byte, for example. In addition, in this example, the information frame inputted into partial decryption equipment 6 from the data transmitter-receiver 4 is also made into the format of drawing 12 (c).

[0045] (A) It is [0046] when data size is expanded by encryption. (a) An example of processing of the partial encryption equipment 5 in ******** is shown in the flow chart of drawing 13 . If the information frame of a format as shown in drawing 12 (a) from which user program 3-1 - 3-m is sent, the input means 51 will input it (step S41), and it will transmit to the encryption control means 52. The encryption control means 52 analyzes the encryption control information section 500 of an information frame (step S42), and sets an analysis result as a control table (step S43).

[0047] For example, the data division 600 which contain five user data U1, U2, U3, U4, and U5 which are 32 bytes, 32 bytes, 16 bytes, 16 bytes, and 16 bytes respectively as shown in drawing 14 (a), If the size of the number and a starting position is for example, 1-byte immobilization in the case of the information frame which consists of the encryption control information sections 500 which specified the user data U3 as a candidate for encryption Since the 66-82nd byte of user data U3 are data for encryption from the head of an information frame and the data before and behind the user data U3 (user data U1, U2, U4, and U5) are not data for encryption For example, the control table 902 with three entries E1, E2, and E3 as shown in drawing 15 is generated, and a starting position, a byte count, and the value illustrated in the column of the existence of encryption, respectively are set up. In addition, at this time, the column of the byte count after encryption is NULL.

[0048] Next, the encryption control means 52 takes out the data of the corresponding part from data division 600 about the entry E2 from which the column of the existence of encryption of the control table 902 is "**", and enciphers them by giving the cryptographer stage 53 (step S44).

[0049] Next, the encryption control means 52 sets the data size after encryption as the column of the byte count after encryption of an entry E2, as shown in drawing 15 (step S45).

[0050] Next, the encryption control means 52 generates the decryption control information section 700 which made the group of the starting position "66" of an entry E2 where the column of the existence of encryption of the control table 902 of drawing 15 is "**", and the byte count after encryption "24" the decryption part assignment information 703 (step S46). Thereby, the decryption control information section 700 shown in drawing 14 (b) is generated.

[0051] Next, from the entry E1 of the control table 902 of drawing 15 , the encryption

control means 52 will stuff into order the original data on the input frame specified in the column of the starting position of the control table 902, and the column of a byte count in the data after encryption if it is "nothing" sequentially from the head of data division, if the column of the existence of encryption of the entry to an entry E3 is "**", and it generates data division 800 (step S47). Thereby, the data division 800 shown in drawing 14 (b) are generated.

[0052] If the information frame which consists of the decryption control information section 700 and data division 800 as mentioned above is generated, the output means 54 will send an information frame to the data transmitter-receiver 4 with the information on destination and delivery origin (step S48).

[0053] (b) An example of processing of the partial decryption equipment 6 in ******** is shown in the flow chart of drawing 16 . If the information frame of a format as shown in drawing 12 (c) from the data transmitter-receiver 4 is sent, the input means 61 will input it (step S51), and it will transmit to the decryption control means 62. The decryption control means 62 analyzes the decryption control information section 700 of an information frame (step S52), and sets an analysis result as a control table (step S53).

[0054] For example, when the inputted information frame is an information frame shown in drawing 14 (b), Since 66-90th byte user data U3' is data for a decryption from the head of an information frame and the data before and behind user data U3' (user data U1, U2, U4, and U5) are not data for a decryption For example, the control table 903 with three entries E1, E2, and E3 as shown in drawing 17 is generated, and a starting position, a byte count, and the value illustrated in the column of the existence of a decryption, respectively are set up. In addition, at this time, the column of the byte count after a decryption is NULL.

[0055] Next, the decryption control means 62 takes out the data of the corresponding part from data division 800 about the entry E2 from which the column of the existence of a decryption of the control table 903 is "**", and decrypts them by giving the decode means 63 (step S54).

[0056] Next, the decryption control means 62 sets the data size after a decryption as the column of the byte count after a decryption of an entry E2, as shown in drawing 15 (step S55).

[0057] Next, the decryption control means 62 generates the encryption control information section 500 which made the group of the starting position "66" of an entry E2 where the column of the existence of a decryption of the control table 903 of drawing 17 is "**", and the byte count after a decryption "16" the encryption part

assignment information 503 (step S56). Thereby, the encryption control information section 500 shown in drawing 14 (a) is generated.

[0058] Next, from the entry E1 of the control table 903 of drawing 17 , the decryption control means 62 will stuff into order the original data on the input frame specified in the column of the starting position of the control table 903, and the column of a byte count in the data after a decryption if it is "nothing" sequentially from the head of data division, if the column of the existence of a decryption of the entry to an entry E3 is "**", and it generates data division 600 (step S57). Thereby, the data division 600 shown in drawing 14 (a) are generated.

[0059] If the information frame which consists of the encryption control information section 500 and data division 600 as mentioned above is generated, the output means 64 will send to the user program of the destination with the information on delivery origin (step S58).

[0060] (B) It is [0061] when data size is not expanded by encryption. (a) An example of processing of the partial encryption equipment 5 in ******** is shown in the flow chart of drawing 18 . If the information frame of a format as shown in drawing 14 (a) from which user program 3-1 - 3-m is sent, the input means 51 will input it (step S61), and it will transmit to the encryption control means 52. The encryption control means 52 analyzes the encryption control information section 500 of an information frame, takes out the data of the part pinpointed by the starting position 501 and byte count 502 from data division 600 (step S62), and enciphers it by giving the cryptographer stage 53 (step S63). Next, the original part of data division 600 is overwritten by the generated code data (step S64). And the output means 54 sends out the information frame by which data division 600 were overwritten to the data transmitter-receiver 4 with the information on destination and delivery origin (S65).

[0062] Thus, when data size is not expanded but it becomes the same size by encryption, the contents of the encryption control information section 500 of the inputted information frame are not changed substantially, but serve as the decryption control information section 700 as it is.

[0063] (b) An example of processing of the partial decryption equipment 6 in ******** is shown in the flow chart of drawing 19 . If the information frame of a format as shown in drawing 12 (c) from the data transmitter-receiver 4 is sent, the input means 61 will input it (step S71), and it will transmit to the decryption control means 62. The decryption control means 62 analyzes the decryption control information section 700 of an information frame, takes out the data of the part pinpointed by the starting position 701 and byte count 702 from data division 800 (step S72), and decrypts it by

giving the decode means 63 (step S73). Next, the original part of data division 800 is overwritten by the generated decode data (step S74). And the output means 64 sends out the information frame by which data division 800 were overwritten to the user program of the destination with the information on delivery origin (S75).

[0064] Thus, when data size is not expanded but it becomes the same size by decryption, the contents of the decryption control information section 700 of the inputted information frame are not changed substantially, but serve as the encryption control information section 500 as it is.

[0065] Although the gestalt of the above operation applied this invention to the encryption to the data transmitted and received between information processors, and a decryption, this invention is applicable also to a record data encryption in case the user program on an information processor enciphers data and records on a local store, and a decryption of the recorded data.

[0066]

[Effect of the Invention] According to this invention, the following effectiveness is acquired as explained above.

[0067] The part which wants to encipher in a series of data can be specified more finely. The reason is that it can specify not only the starting position of data to encipher among a series of data but its die length, and is because a starting position and two or more sets of die length can be specified.

[0068] Thus, since a part to encipher can be specified finely, necessary minimum encryption is attained and large compaction of the encryption processing time is attained.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing an example of the information processor which applied this invention.

[Drawing 2] It is the block diagram showing the example of a configuration of partial encryption equipment.

[Drawing 3] It is the block diagram showing the example of a configuration of partial decryption equipment.

[Drawing 4] It is drawing showing an example of a format of an information frame.

[Drawing 5] It is the flow chart which shows the example of processing of partial encryption equipment.

[Drawing 6] It is drawing showing the example of an information frame.

[Drawing 7] It is drawing showing the example of the control table which partial encryption equipment uses.

[Drawing 8] It is the flow chart which shows the example of processing of partial decryption equipment.

[Drawing 9] It is drawing showing the example of the control table which partial decryption equipment uses.

[Drawing 10] It is the flow chart which shows the example of processing of partial encryption equipment.

[Drawing 11] It is the flow chart which shows the example of processing of partial decryption equipment.

[Drawing 12] It is drawing showing the example of a format of an information frame.

[Drawing 13] It is the flow chart which shows the example of processing of partial encryption equipment.

[Drawing 14] It is drawing showing the example of an information frame.

[Drawing 15] It is drawing showing the example of the control table which partial encryption equipment uses.

[Drawing 16] It is the flow chart which shows the example of processing of partial decryption equipment.

[Drawing 17] It is drawing showing the example of the control table which partial decryption equipment uses.

[Drawing 18] It is the flow chart which shows the example of processing of partial encryption equipment.

[Drawing 19] It is the flow chart which shows the example of processing of partial decryption equipment.

[Drawing 20] It is the explanatory view of the conventional trouble.

[Description of Notations]

1 -- Information processor

2 -- Communication line

3-1 - 3-m -- User program

4 -- Data transmitter-receiver

5 -- Partial encryption equipment

6 -- Partial decryption equipment

7 -- Record medium

51 61 -- Input means

52 -- Encryption control means

53 -- Cryptographer stage

54 64 -- Output means

62 -- Decryption control means

63 -- Decode means